Hogan Lovells

Government Contracts Guide

for Space and Satellite Companies

Authors

Mike Mason
Partner | Washington, D.C.
mike.mason@hoganlovells.com

Stacy Hadeka
Partner | Washington, D.C.
stacy.hadeka@hoganlovells.com

Mike Scheimer
Partner | Washington, D.C.
michael.scheimer@hoganlovells.com

Lauren Colantonio
Associate | Washington, D.C.
lauren.colantonio@hoganlovells.com

Additional Space and Satellite Team Contacts

Randy Segal
Partner | Northern Virginia, Silicon Valley, Washington, D.C.
randy.segal@hoganlovells.com

Steven Kaufman
Partner | Washington, D.C.
steven.kaufman@hoganlovells.com

Alexis Sáinz
Partner | Washington, D.C.
alexis.sainz@hoganlovells.com

Stephen Propst
Partner | Washington, D.C.
stephen.propst@hoganlovells.com

Ari Fitzgerald
Partner | Washington, D.C.
ari.fitzgerald@hoganlovells.com

Gerry Oberst
Sr. Counsel | Washington, D.C.
gerry.oberst@hoganlovells.com

George John
Sr. Associate | Washington, D.C.
george.john@hoganlovells.com

Ryan Thompson
Sr. Associate | Washington, D.C.
ryan.thompson@hoganlovells.com

Table of contents

Space plays a critical role in American security, prosperity, and way of life. Space-based services support the world's financial, information, and communications systems, scientific discoveries, and environmental monitoring. Americans benefit from space-based services every day. Increasingly, national and Department-level guidance and strategy reflect the centrality of space to U.S. national security and to the U.S. economy, as well as the growing threats to the domain.

U.S. Department of Defense, Space Policy Review and Strategy on Protection of Satellites, September 2023, at 4.

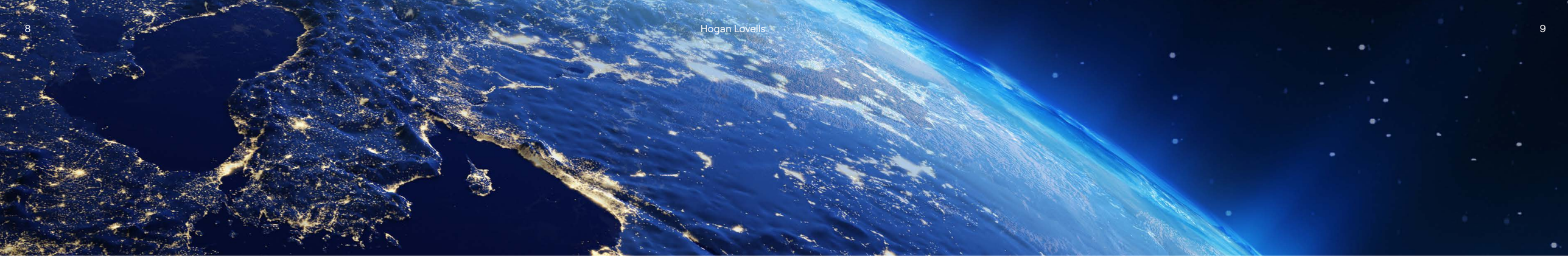
Introduction

The space domain is indeed central to U.S. national security and economic interests. The importance of space-based activity continues to grow significantly, and the opportunities for advancement of the space industry have never been greater. Record government and private sector funding are driving opportunities for major scientific and technological breakthroughs with implications for commercial, scientific, and national security capabilities. The Federal Government market presents opportunities for both traditional and non-traditional aerospace and defense companies, as well as academic institutions. Government-funded space-related programs span from those focused on basic and applied research through to the procurement and operation of spacecraft, related ground systems, and space-related services. The opportunities flow through the supply chain, including to lower-level suppliers that are on the cutting edge of technologies such as additive manufacturing, advanced materials, artificial intelligence, biotechnology, next generation communications and sensing capabilities, and propulsion. Government funding continues to be strong even while the growth in private capital investments has leveled somewhat.[1] For fiscal year 2025, the U.S. Department of Defense's (DoD's) budget request includes $33.7 billion for space programs. The request includes, among other things, $2.4 billion for space launch capabilities; $1.5 billion for more resilient position, navigation and timing; and $4.2 billion for more resilient and protected satellite communications. The request also includes $4.7 billion to develop new missile warning and tracking architectures and $12.3 billion for a range of other capabilities aimed at increasing the resiliency of DoD's existing space architectures.[2]

Additionally, the Government is increasingly opening its programs to organizations that are not traditional government contractors. Indeed, the 2024 DoD Commercial Space Integration Strategy reflects DoD's plan to pursue the following top-level priorities to maximize the benefits of integrating commercial space solutions into national security architectures: (1) Ensure access to commercial solutions across the spectrum of conflict; (2) Achieve integration prior to crisis; (3) Establish the security conditions to integrate commercial space solutions; and (4) Support the development of new commercial space solutions for use by the joint force. Moreover, the U.S. Space Force recently issued its Commercial Space Strategy that "[w]hen feasible and cost effective, [the Space Force] will integrate commercial space solutions into existing doctrine, strategy, concepts, force designs, acquisitions, and operations."[3] Accordingly, the opportunities for access to the U.S. Government space market continues to grow.

Although government contracts and other forms of government funding are often critical to a space industry participant's success, there are associated risks and compliance obligations that a market participant will need to address. For example, government contracts are often subject to unique competition requirements and non-negotiable terms and conditions, including those relating to the Government's unilateral right to terminate the agreement for its convenience, intellectual property, cost allowability, warranties, and audits. Risk mitigation measures that are common in the commercial market are often unavailable in the government market. Government contractors and subcontractors are also subject to a variety of unique compliance requirements pertaining to supply chains, cybersecurity, business conduct and ethics, and affirmative action for certain disadvantaged groups. Thus, while government contracts and funding can offer lucrative opportunities, they also come with unique challenges that may require specialized expertise and resources to navigate successfully.

This Guide provides an overview of the government market for companies and educational institutions that participate, or wish to participate, in government funded space-related activity. Below we identify and discuss the main government customers, the distinctions in the types of government agreements and terms, and the most prominent compliance requirements for government contracting.



Key Government Customers

The Government's consumption and funding of space-related activity comes from a variety of government agencies. Government customers for space-related products and services include civilian, defense, and intelligence community customers. The "target government customer" for a space company will largely depend on matching a company's goods and services to the appropriate government mission and contracting vehicle set. To aid in that process, the following provides a brief overview of the largest government consumers and funders of space activity.

U.S. National Aeronautics and Space Administration (NASA): NASA is the U.S. Government civilian agency that is synonymous with supporting space research and exploration from a civilian perspective. NASA's responsibilities include space exploration, development of space technology, earth and space science, and aeronautics research.[4] Major NASA programs include deep space exploration (including the Artemis lunar exploration program and the Mars campaign); space operations (*e.g.*, International Space Station, space transportation, and commercial development of low earth orbit); space technology development; science endeavors (*e.g.*, earth science, planetary science, and astrophysics); and aeronautics (fuel technologies, aircraft noise, and high-speed commercial flight).[5] NASA's budget request for fiscal year 2025 is $25.4 billion.

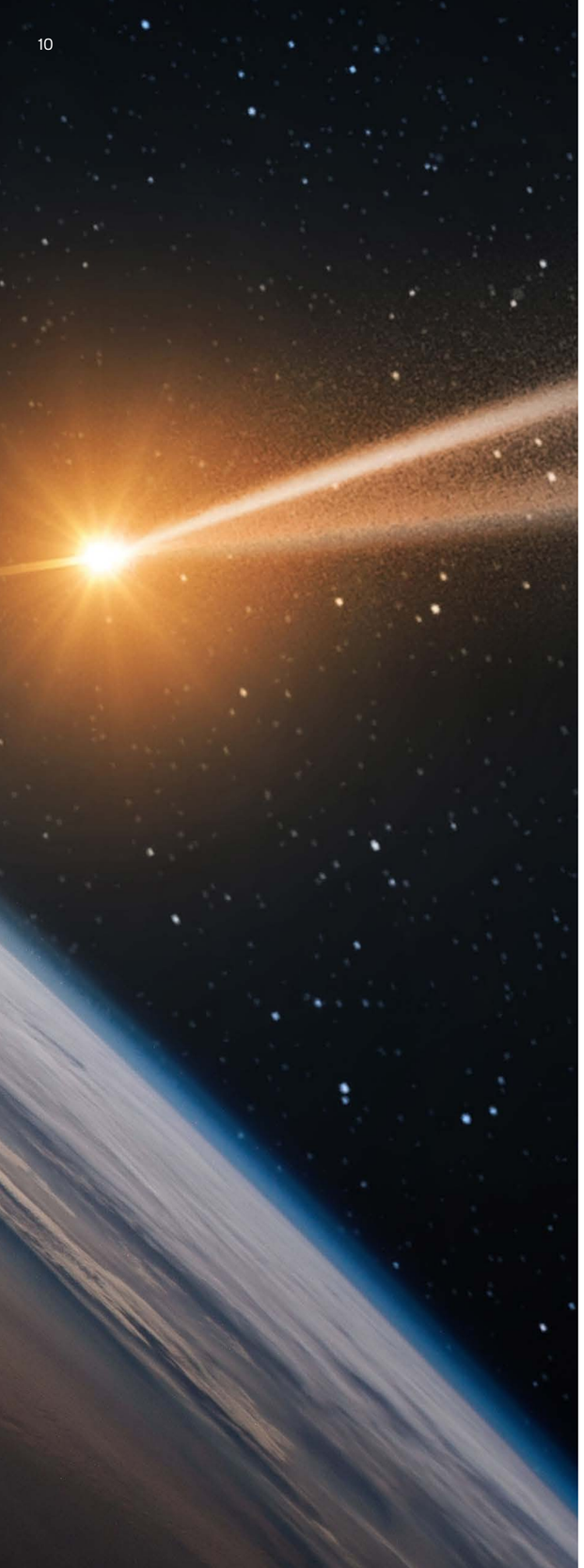
U.S. Space Force: The creation of the U.S. Space Force in December 2019 denotes an inflection point for the strategic importance that the United States places on the space domain. Although a separate branch of the military, the Space Force is situated under the Department of the Air Force in a manner similar to the Marine Corps' organization under the Department of the Navy. The Space Force is tasked with ensuring a comprehensive and integrated approach to national security, including threats to and from adversary space systems.[6] The Space Force's responsibilities (including those of its Space Development Agency, Space Systems Command, Space Rapid Capabilities Office, and Commercial Satellite Communication Office) include launches of satellites and other spacecraft, satellite operations, space-based communications, surveillance of the space environment, satellite defense, and missile warning systems.[7] The Space Force also supports research and development activity to advance launch capability, satellite technology, space situational awareness, and other space-related capabilities. As reflected in its Commercial Space Strategy released in April, 2024, the Space Force is increasingly turning to commercial providers to leverage commercial technologies and rapid development cycles. Under the Space Force's recently articulated strategy, mission areas considered for commercial support are subdivided into the following categories:

- Space Domain Awareness
- Satellite Communications
- Space Access (including Launch), Mobility, and Logistics
- Tactical, Surveillance, Reconnaissance, and Tracking
- Space-based Environmental Monitoring
- Cyberspace Operations
- Command and Control
- Positioning, Navigation, and Timing
- Hybrid Space Mission Enablers, meaning those functions that span multiple missions and are fundamental to conducting space operations[8]

SpaceWERX: Considered the "Innovation Arm of the U.S. Space Force," SpaceWERX is aligned both with the Space Force and the Air Force Research Laboratory, or AFWERX. Similar to AFWERX's mission to develop innovative ecosystems, SpaceWERX aims to expand the space industrial base through research and development and civil-military collaborations that promote commercial investment in the newest space technologies. Many SpaceWERX programs bring together innovative companies, including small businesses, with government communities to quickly field space systems. SpaceWERX often invests in dual-use technologies to accelerate government space capabilities.[9]

Defense Innovation Unit (DIU): DIU is a DoD organization focused on fielding and scaling commercial technology across the U.S. military on commercial terms, at speeds that typically are much faster than those experienced with traditional government contracts. DIU aims to assist its internal DoD customers by lowering barriers for commercial companies in the defense market. This is often accomplished through the DIU's use of Other Transaction (OT) agreements (discussed further below) as an entry point for commercial market companies, paving the way for larger-scale defense contracts.

Defense Advanced Research Projects Agency (DARPA): DARPA is another DoD organization that focuses on the military's advancement of newer technologies. Part of DARPA's stated mission is to make pivotal investments in breakthrough technologies for national security. DARPA dates this mission to the former Soviet Union's launch of the first artificial satellite, Sputnik, in 1957, which spurred the United States to commit to being "the initiator and not the victim of strategic technological surprises."[10]



DARPA also relies often on OT agreements to pursue break-through technologies, and has used them on impactful programs such as:

- Laser Communications
- Experimental Space Plane
- Robotic Servicing of Geosynchronous Satellites (RSGS)[11]

More recently, in September 2023, DARPA announced that it "is seeking innovative concepts from small businesses and nontraditional defense contractors in the technical domain of space superiority."[12]

Intelligence Community: Agencies such as the National Reconnaissance Office (NRO), National Geospatial-Intelligence Agency (NGA), National Security Agency (NSA), and Intelligence Advanced Research Project Activity (IARPA) are also key supporters and consumers of space activity. For example, the NRO develops and purchases launch services, space-based assets, and ground systems to identify threats around the world. The NGA analyzes space-based imagery of earth and distributes intelligence to its internal governmental customers. As a whole, the U.S. intelligence community and DoD are increasingly procuring imagery from operators of commercial satellites.[13]

Department of Commerce, National Oceanic and Atmospheric Agency (NOAA): NOAA engages industry through several space-related programs, including satellite monitoring of both earth and space-based weather and space traffic coordination.

It should be emphasized that the consumption of space-related goods and services extends beyond the above-named agencies. For example, the Departments of Agriculture, Energy, and Interior have all procured data from commercial satellite imagery contracts.[14] Also, the Departments of the Army and Navy, and the Missile Defense Agency, are all strong consumers of space-related goods and services.

Basic Government Contract Types

The payment terms, compliance obligations, and degree of risk to space organizations in their government contracting endeavors will depend in part on the type of agreement used to procure or fund the goods or services. Traditional government contracts are governed by the requirements set forth in 48 C.F.R. Part 15 (Federal Acquisition Regulation (FAR) Part 15). These types of contracts typically impose the most compliance obligations and are least consistent with standard commercial practices. Contracts for commercial products and services are often governed by FAR Part 12, which imposes terms and conditions that are intended to be (but are often not) consistent with standard commercial practice. OT agreements, Space Act agreements, Small Business Innovation Research (SBIR)/ Small Business Technology Transfer (STTR) (commonly referred to as "SBIR/STTR"), and grants/cooperative agreements impose their own obligations, which are often less burdensome than contract types governed by either FAR Part 15 or FAR Part 12. With limited exceptions, and regardless of agreement type, terms that would provide for open-ended indemnification flowing from the Government to the contractor are unavailable due to fiscal law constraints.

FAR Part 15 Contracts

FAR Part 15 governs negotiated procurements, *i.e.*, "traditional" government contracts awarded generally pursuant to competitive proposals. These procurements usually involve a formal solicitation document and are awarded on a "best value" basis after considering factors such as technical merit, past performance, and price.

The FAR Part 15 terms and conditions are imposed through a variety of contract clauses that often include terms that are inconsistent with a contractor's commercial practice. For example, FAR Part 15 warranty terms may differ materially from the contractor's standard commercial warranty terms. As far as intellectual property, if the Government funds the development of the technical data or computer software under the contract, the Government will receive broad rights to disclose and use the technical data or software, including a right to disclose the data to other contractors and permit those contractors to use the data. Contract pricing may be cost reimbursable, fixed price, time and materials, labor hour, or an incentive type. If the contract is cost-based, the contractor will be subject to rules that govern the costs that are allowed to be charged to the Government (depending on dollar value and extent of government cost-based business, these will include the Cost Principles, Cost Accounting Standards, and the so-called Business Systems rules). Also, regardless of whether the contract is FAR Part 15 or FAR Part 12, the contract will include a government right to terminate the contract for its convenience, in which case the contractor generally receives reimbursement for supplies delivered/ services performed and accepted, plus any additional costs incurred in performance.

FAR Part 12 Contracts

FAR Part 12 sets forth regulations applicable to procurement contracts for commercial services and products. For these commercial acquisitions, the regulations prescribe firm-fixed-price contracts or fixed-price contracts with economic price adjustment. Products and services that are generally available to the public in the same form or with minor modifications typically qualify as "commercial" and are suitable for FAR Part 12 treatment. Additionally, contracting officers within DoD have discretion to offer FAR Part 12 contracting terms (rather than the more onerous FAR Part 15 terms) to "non-traditional defense contractors," including in situations where the products or services offered would not otherwise qualify as "commercial."[15]

FAR Part 12 contracts can be awarded using streamlined acquisition procedures and with fewer regulatory requirements. The basic FAR Part 12 terms and conditions are set out in a specific FAR clause (FAR 52.212-4), and those requirements are intended to be consistent with standard commercial practices. For example, under FAR 52.212-4, a modification to the contract requires the parties' *mutual* agreement. In contrast, FAR Part 15 contracts include a Changes clause that allows the Government to *unilaterally* change many aspects of the contract (with a cost adjustment to contract price, if necessary). Also, FAR Part 12 contracts benefit from greater intellectual property protection, and contractors may generally use standard commercial licenses and warranties. Also, the Government does not have the right to demand "certified cost or pricing data" under Truthful Cost or Pricing Data requirements and FAR 15.403-1. For subcontractors, it is important to note that the regulations exempt subcontractors of commercial products and services from many of the mandatory FAR flow-down clauses.

Other Transaction Agreements

OT agreements are legally binding instruments between the U.S. Government and industry or academia for a broad range of research and prototyping activities. OT agreements are more consistent with commercial contracting practices than either FAR Part 15 or FAR Part 12 contracts. The purpose of OT agreements is to provide the Government with greater flexibility to adopt commercial practices and terms to better gain access to leading technologies. Although the U.S. Government's authority to enter into OT agreements has existed in various forms since 1958, relatively recent legislative developments and the DoD's establishment of the DIU have generated a significant increase in interest by both government agencies and government contractors.

OT agreements typically are defined by what they are not. The rules applicable to standard procurement contracts (e.g., the FAR and FAR Supplements), grants, and cooperative agreements are generally inapplicable. Instead, the parties to an OT agreement have significant flexibility to negotiate the terms that address intellectual property rights, changes/modifications, terminations/cancellations, payment timing, accounting system, and other requirements. Thus, OT agreements are commonly viewed much more favorably than FAR-based contracts by both traditional and non-traditional contractors, although certain cost sharing requirements may apply to traditional government contractors (depending on their OT teaming arrangements). Moreover, because the FAR and Competition in Contracting Act do not apply to the award of an OT agreement, the evaluation process can be significantly streamlined and at least partially insulated from bid protest challenges. Another benefit is that follow-on production agreements may be awarded without competition if certain conditions relating to prototype OT agreements are met.

NASA Space Act Agreements

NASA has broad discretionary authority to carry out its unique functions, thanks to the National Aeronautics and Space Act (Space Act).[16] The Space Act provides NASA's authority to enter into flexible contracts, cooperative agreements, and OTs as necessary to conduct business with nontraditional government contractors to swiftly deliver technical space-based capabilities in a rapidly evolving environment.[17] NASA's OTs, commonly referred to as Space Act Agreements, or SAAs, are not subject to the FAR and its rigid constraints. NASA can further tailor SAAs by offering Reimbursable Agreements, Nonreimbursable Agreements, Funded Agreements, or International Agreements.[18]

Reimbursable Agreements are those agreements in which NASA's costs associated to the activity are reimbursed by the Agreement Partner (in full or in part). NASA enters into Reimbursable Agreements when it has unique goods, services, and facilities that are not currently being fully utilized to accomplish mission needs, allowing the Agreement Partner to advance its own interests. These Reimbursable Agreements may be made available to others on a noninterference basis and consistent with the Agency's missions and policies. Nonreimbursable Agreements are those that involve NASA and one or more Agreement Partners in a mutually beneficial activity that will further the Agency's Missions. Unlike Reimbursable Agreements, each

partner bears the cost of its participation, and no funds are exchanged between the parties. NASA relies on Nonreimbursable Agreements for the agency to offer its expertise or facilities for use. NASA separately uses Funded Agreements when appropriated funds are transferred to a domestic Agreement Partner to accomplish an Agency Mission. Funded Agreements may be used only when the Agency's objective cannot be accomplished using a procurement contract, grant, or cooperative agreement, meaning a Funded Agreement will not support the acquisition of goods and services. A Funded Agreement uses appropriated funds to meet NASA's statutory objectives as set forth in 51 U.S.C. § 20102. Last, International Agreements, which can either be Reimbursable or Nonreimbursable Agreements, are entered into when the Agreement Partner is a foreign entity. A foreign partner may be a legal entity not established under a state or Federal law of the United States and may include a commercial or noncommercial entity or person or governmental entity of a foreign sovereign.

Technology Investment Agreements, Cooperative Agreements, and Grants

Technology investment agreements, cooperative agreements, and grants are not procurement contracts for goods or services but government agreements that promote research and development in furtherance of the public good. Investment in commercial research and development is paramount to meet the military's space objectives, and within the U.S. Space Force alone, research, development, testing, and engineering (RDT&E) funding often outsizes funding allocated to programs associated with traditional procurement, maintenance and operations. Because the commercial sector can keep pace with the rapidly evolving space ecosystem, the government needs creative and flexible research and development vehicles.

Technology Investment Agreements (32 CFR Part 37)

Technology Investment Agreements (TIAs) are not government contracts but federal assistance instruments, namely cooperative agreements, that stimulate or support research with the help of the Government's substantial involvement.[19] DoD TIAs are subject to the DoD Grant and Agreement Regulations (DoDGARs) under 32 C.F.R. Parts 21 and 37.[20] The DoD relies on TIAs to reach its simultaneous goals of developing the best and most sophisticated technologies for defense needs and fostering strong civil-military relationships. TIA funding further reduces barriers to participation in defense research, promotes government and commercial relationships across the defense industrial base, and encourages funding recipients to develop best business practices.[21] The DoD relies on TIAs when other funding instruments are not conducive to these goals.

Grants and Cooperative Agreements

Grants and cooperative agreements are also available to fund space activity, especially with respect to space-related research. Grants and cooperative agreements are a form of federal assistance agreements to carry out a public purpose (e.g., research) and support or stimulate an activity. The major difference between grants and cooperative agreements is that grants do not anticipate substantial involvement between the sponsoring agency and the recipient during performance of the contemplated activity, whereas cooperative agreements may require it. In contrast to grants and cooperative agreements, the principal purpose of a FAR-based procurement contract is to acquire goods or services for the direct benefit of the Government. Notably, recipients of grants and cooperative agreements typically have less precise milestones and deliverables outlined in procurement contracts. Grants and cooperative agreements typically require "best efforts" in research, rather than the delivery of promised goods or the acceptance of completed performance of services. Moreover, grant and cooperative agreements are subject to the more flexible requirements of the Office of Management and Budget's Guidance for Federal Financial Assistance under Title 2 of the C.F.R. Grants and cooperative agreements, however, are typically cost reimbursement awards, which subject for-profit organizations to the same FAR cost principles that apply to Federal contractors under cost reimbursable procurement contracts.

Small Business Innovative Research (SBIR)/Small Business Technology Transfer (STTR) Contracts and Grants

The Government has a vested interest in increasing small business participation in research and development (R&D) and does so through the well-known SBIR/STTR set-aside programs. These programs explore R&D related to critical defense priorities. Under the Small Business Innovative Research (SBIR) program, certain federal agencies allocate a portion of funding to a multi-phase R&D grant program, awarding small businesses with grants or contracts that stimulate innovation, increase

small business participation in R&D, and expand private sector commercialization of government funded R&D. The Small Business Technology Transfer (STTR) program places an additional emphasis on allocating intellectual property rights for continued R&D research.[22] SBIR/STTR programs are unique and allow small businesses to key in on defense priorities. For example, SpaceWERX's SBIR program encourages small businesses to explore their capabilities by partnering with Space Force units. Its STTR program focuses on developing technology for both military and commercial use. All SBIR/STTR programs are similarly structured and comprised of three phases: Phase I funds R&D specific to agency requirement; Phase II continues funding to explore specific program needs that have commercial application potential; and Phase III focuses on commercial or government application but no longer relies on SBIR funding.

Risk-Mitigation Terms and Conditions

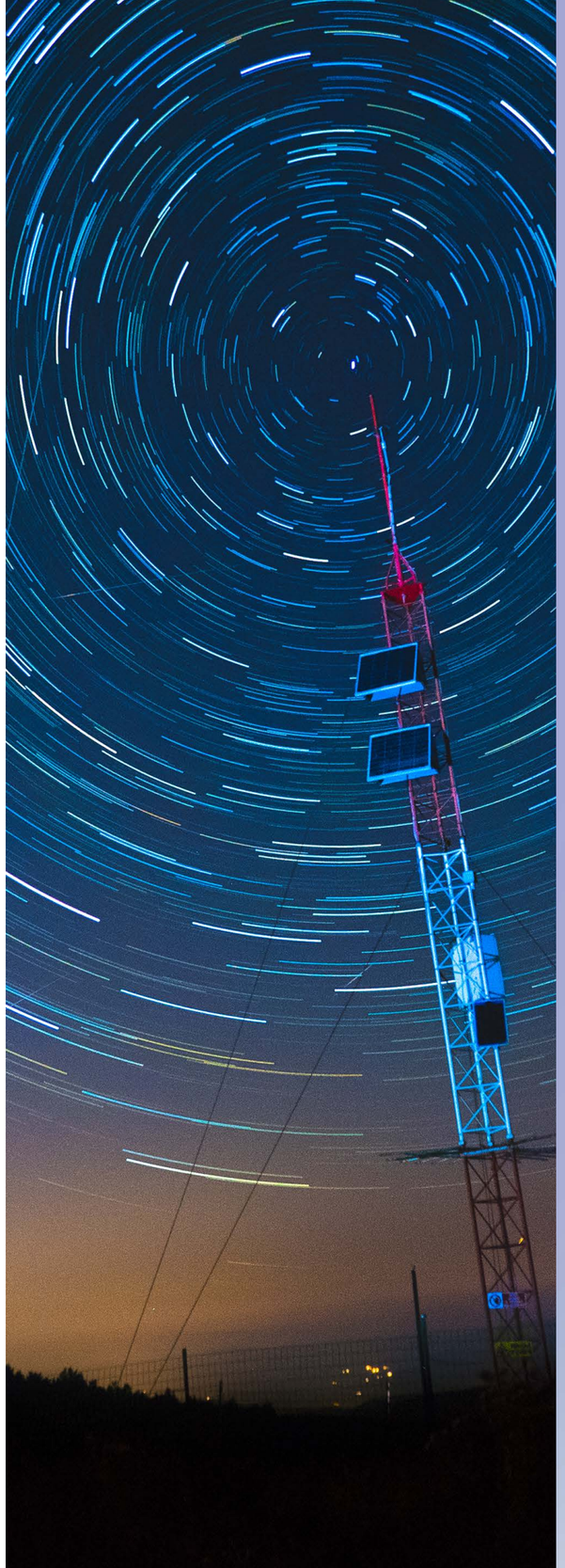
Space companies perform many types of activities that pose heightened risk of loss to property or harm to persons. This is especially true for those activities relating to the use of solid or liquid high energy propellant for launch and spacecraft propulsion, the use of nuclear energy to power spacecraft, re-entry related risks, the potential for on-orbit collisions, and the possibility of loss of human life for anomalous performance of space transportation services. Additionally, there may be some activities where it is difficult for the contractor to obtain insurance due to the classified nature of the program. As reflected in the Department of Defense's Commercial Space Integration Strategy, current possibilities for financial protection of contractors include commercial insurance, commercial war-risk insurance, U.S. Government-provided insurance (currently available only for air and maritime domains), and indemnification.

The following presents some of the unique risk-mitigation considerations for companies that are under contract with the Government or one of its contractors.

Indemnification Protections

In commercial contracting, contractual indemnification often serves as an important tool for mitigating risks that are deemed to be hazardous. There are some activities that a company may forego completely due to their hazardous nature and lack of adequate insurability. Regarding government contracts, the general rule is that the Government may not enter into indemnification agreements with its contractors due to constraints posed by fiscal law, specifically the Anti-Deficiency Act.[23] This statute prevents federal agencies from entering into contracts or obligations that may surpass or precede available appropriated funds. Essentially, the Government is barred from entering uncapped indemnification agreements unless expressly authorized by Congress.

Importantly, there are a number of such exceptions authorized by Congress that are relevant to space companies and organizations. As discussed below, activities that "facilitate the national defense" but pose risks that are unusually hazardous or nuclear in nature may be eligible for indemnification coverage from the Government under Public Law 85-804 or its sister provision for research



and development efforts under 10 U.S.C. § 3861. Additionally, NASA has statutory authority under 51 U.S.C. § 20148 covering claims by third parties for death, bodily injury, or loss of or damage to property resulting from "launch services and reentry services carried out under the contract that the contract defines as unusually hazardous or nuclear in nature."[24] These indemnification coverages are separate and distinct from indemnification coverage under the Commercial Space Launch Competitiveness Act provided by the Federal Aviation Administration.[25] (NASA, however, may also agree to license launch and reentry under the FAA licensing and indemnification regime, including indemnification coverage.)

Public Law 85-804 Indemnification

Pub. Law 85-804 grants the President the ability to authorize federal agencies to indemnify contractors against risks that are "unusually hazardous or nuclear" in nature.[26] Under this statute and its implementing regulations, FAR Subpart 50.1 – Extraordinary Contractual Actions, the Government may indemnify a contractor where its performance involves risks that are unusually hazardous or nuclear in nature and for which insurance coverage is unavailable at a reasonable cost.[27] In general, to apply for such coverage the contractor must provide the Government with a description of the unusually hazardous or nuclear risks associated with the project and detailed information regarding available insurance coverage. The contractor must explain why the risk is nuclear in nature or *unusually* hazardous, not just hazardous. Ultimately, the Secretary of the cognizant agency must determine that the indemnity is necessary "to facilitate the national defense," which is a determination that is discretionary

and made on a case-by-case basis. If granted, the indemnification will cover:

- Claims (including reasonable expenses of litigation or settlement) by third persons (including employees of the contractor) for death; personal injury; or loss of, damage to, or loss of use of property;
- Loss of, damage to, or loss of use of contractor property, excluding loss of profit; and
- Loss of, damage to, or loss of use of government property, excluding loss of profit.[28]

The indemnification coverage applies only to the extent that the claim, loss, or damage arising out of the risk defined in the contract as unusually hazardous or nuclear in nature is not compensated by insurance or otherwise.[29]

Indemnification under 10 U.S.C. 3861

Like Public Law 85-804 indemnification, DoD may indemnify contractors engaged in research and development projects for third party claims and loss or damage to contractor or government property arising from a risk that the contract defines as unusually hazardous. The indemnification is for amounts in excess of insurance coverage. The regulations recognize that there may be contracts that include work covered by both 10 U.S.C. 3861 and Public Law 85-804. In those cases, Public Law 85-804 will apply only where 10 U.S.C. 3861 does not apply.[30]

Indemnification for NASA Launch Services and Reentry Services

In addition to Public Law 85-804, NASA has available the indemnification framework under 51 U.S.C. § 20148. This indemnification coverage is similar to the coverage available under Public Law 85-804. The indemnification coverage encompasses claims that may originate from *launch services and reentry services* carried out under the contract that the contract defines as unusually hazardous or nuclear in nature. Notably, like the Federal Aviation Administration's authority, this NASA authority requires a reciprocal waiver of claims. That is, each party to the waiver agrees to be responsible, and agrees to ensure that its related entities are responsible, for damage or loss to its property, or for losses resulting from any injury or death sustained by its employees or agents, as a result of activities arising out of the performance of the contract.

Other Risk Mitigation Provisions

Based on the risk-profile of each project and contract type, contractors will want to consider potentially available terms and conditions as part of its risk-mitigation strategy. The following briefly discusses several contract provisions that may be leveraged to mitigate certain risks.

FAR Part 12 Disclaimer of Consequent Damages

The standard clause applicable to FAR Part 12 contracts for commercial products or services, FAR 52.212-4(p), provides that the contractor will not be liable (except as provided by an express warranty) to the Government for *consequential* damages resulting from any defects or deficiencies in *accepted* items. This disclaimer of consequential damages applies only to accepted products and services. FAR Part 12, however, permits the parties to tailor certain provisions, including this one. For example, the provision may be tailored (subject to government agreement) to disclaim consequential damages for both accepted and unaccepted items.

FAR 52.228-7– Insurance – Liability to Third Persons

In *cost-reimbursement* contracts, the Government typically self-insures for liability to third parties above and beyond that covered by contractually-required insurance by inserting the clause at FAR 52.228-7– "Insurance – Liability to Third Persons." Under this clause, a contractor is reimbursed not only for the cost of the insurance expressly required for the contract, but also for uninsured liabilities for loss of or damage to property (other than property owned or used by the contractor) or death or bodily injury to third persons arising out of contract performance. However, unlike Public Law 85-804 indemnification, this reimbursement is subject to the availability of appropriated funds at the time the liability arises.

FAR Subpart 46.8 – Contractor Liability for Loss of or Damage to Property of the Government

For FAR Part 15 (non-commercial) contracts, the Government will also generally act as self-insurer by relieving contractors of liability for loss of or damage to property of the Government that (1) occurs *after acceptance* of supplies delivered or services performed under a contract and (2) results from defects or deficiencies in the supplies or services. However, the Government generally will not relieve the contractor of liability for loss of or damage to the contract end item itself, *except for high value items*. General exceptions to the limitation of liability include: (i) to the extent the contractor's liability is expressly provided in the contract; (ii) when a defect or the Government's acceptance results from willful misconduct or lack of good faith on the part of the contractor's management; or (iii) to the extent the loss to the Government is covered by the contractor's insurance.

Potentially applicable clauses are located at FAR 52.246-23 (Limitation of Liability), FAR 52-246-24 (Limitation of Liability – High-Value Items), and FAR 52.246-25 (Limitation of Liability—Services).

FAR Part 45 Government Property Clauses

Where the clause located at FAR 52.245-1, Government Property, is included in the contract, the contractor *generally* is not liable for loss or destruction of, or damage to, the government property (including contractor acquired or fabricated property) or incidental expenses in excess of any insurance required to be maintained under the contract. Exceptions include where the loss or damage results from willful misconduct or lack of good faith of the contractor's managerial personnel or the failure of the contractor's managerial personnel to establish and administer a program or system for administering and protecting the property. Note that there are subtle differences with respect to the clause's applicability and impact on fixed-price contracts depending on whether the government agency is a DoD or non-DoD agency.

Government Contractor Defense

The "government contractor defense" may work to protect a government contractor from tort liability arising from compliance with specifications provided by or approved by the Government. The doctrine has its modern origins in the U.S. Supreme Court's decision in *Boyle v. United Techs. Corp.*,[31] where the Court adopted a three-part test to determine applicability: "Liability for design defects in military equipment cannot be imposed, pursuant to state law, when (1) the United States approved reasonably precise specifications; (2) the equipment conformed to those specifications; and (3)

the supplier warned the United States about the dangers in the use of the equipment that were known to the supplier but not to the United States."[32] With respect to the first element of the test, it is important to note that "the government's approval of a particular specification must be more than a cursory rubber stamp approving the design . . . . [r]ather, approval must result from a continuous exchange and back and forth dialogue between the contractor and the government."[33] Thus, "[w]hen the government engages in a thorough review of the allegedly defective design and takes an active role in testing and implementing that design, [the] first element is met."[34]

Since *Boyle*, courts have wrestled with questions such as whether the defense only applies to military contractors and whether it applies to contractors that are providing the Government with services (rather than equipment or goods). On the first point, "many . . . courts have extended the defense's availability to also protect nonmilitary contractors from liability arising out of federal procurement and services contracts for civilian projects."[35] For example, the Third Circuit has explained that "the government contractor defense is available to nonmilitary contractors . . . . It is the exercise of discretion by the government in approving a product design, and not whether the product was military or nonmilitary in nature, which determines whether the government contractor defense is appropriate."[36] The Eleventh Circuit has also considered the defense in a nonmilitary context, *i.e.*, a case involving a vaccine manufacturer, and has concluded that "[b]oth the history of the defense and its general rationale lead us to the conclusion that it would be illogical to limit the availability of the defense solely to 'military' contractors. If a contractor has acted in the sovereign's stead and can prove the elements of the defense, then he should not be denied the extension of sovereign immunity that is the government contract defense."[37] The Seventh Circuit has reached similar conclusions.[38] In contrast, the Ninth Circuit has repeatedly limited the defense to military contractors.[39] With respect to whether the defense applies to contracts for services (as opposed to only those for goods/equipment), the Eleventh Circuit and the D.C. Circuit are among those that have concluded it does.[40] Although the Ninth Circuit has not yet explicitly addressed this question, several California district court decisions have agreed that the defense is not limited to equipment contracts (with at least one court adopting a contrary view).[41]

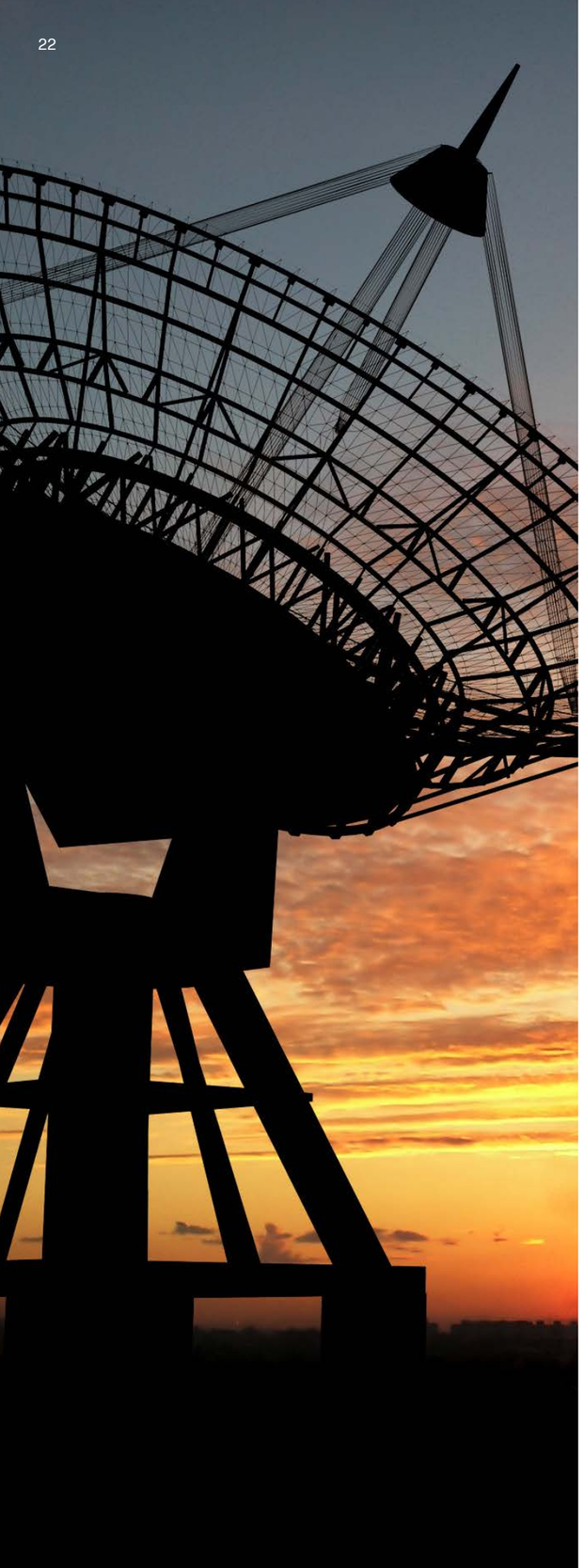
Compliance Obligations

Space companies and organizations that enter contracts with the Government are subject to many government-unique compliance obligations. The DoD's Commercial Space Integration Strategy, for example, expressly recognizes that "[c]ontracts and other agreements will address the cyber, data, and supply chain security requirements that commercial entities will need to meet to work with the Department."[42] Compliance with these obligations require appropriate controls and processes to ensure that the contractor does not run afoul of the government requirements. Noncompliance can have serious consequences, including liability up to three times damages and significant civil penalties under the False Claims Act (31 U.S.C. §§ 3729-3733). In severe cases, noncompliance may result in suspension or debarment from government contracting.[43] The following discussion focuses on several of the most notable compliance areas.

Cybersecurity

Space assets are prime targets for cyber-attacks given their importance to national security, economic, and scientific endeavors. As such, space companies require awareness of heightened cyber protections in their systems, processes, and information technology. This point has been repeatedly emphasized by the U.S. Government. For example, Space Policy Directive-5 has emphasized the importance of "[p]rotection against communications jamming and spoofing, such as [through] signal strength monitoring programs, secured transmitters and receivers, authentication, or effective, validated, and tested encryption measures designed to provide security against existing and anticipated threats during the entire mission lifetime."[44] In addition to cybersecurity requirements that may be included in a government contract's specifications or statement of work, space and other companies that conduct business with the Government are subject to a growing number of substantial cybersecurity requirements aimed at protecting the company's systems that house government data.

There are aggressive cybersecurity compliance obligations imposed by both DoD and civilian agencies. The ability of a space company to comply with the applicable standards and otherwise safeguard sensitive government information is important for competing for new government contracts and avoiding liability associated with a data breach and/or alleged misrepresentations of compliance. At the most basic level, FAR clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, applies to contracts where the contractor or subcontractor may have "Federal



Contract Information" (FCI) residing in or transiting through its information system.[45] This clause requires contractors to safeguard contract information systems that process, store, or transmit FCI and identifies 15 security requirements for safeguarding those systems.

Regarding DoD contracts, such contracts will include Defense FAR Supplement (DFARS) clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, which imposes safeguarding requirements for Covered Defense Information (CDI) and requirements for cyber incident reporting. This clause applies to all DoD contractors and subcontractors, except for contracts for the acquisition *solely* of commercially available off-the-shelf (COTS) items. Contractors and subcontractors are required to provide "adequate security" on all covered contractor information systems. This obligation includes implementation of 110 security requirements contained in National Institute of Standards and Technology (NIST) Special Publication ("SP") 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." The NIST requirements go well beyond the relatively limited number of requirements set out in FAR clause 52.204-21. The clause also requires that the contractor meet Federal Risk and Authorization Management Program (FedRAMP) standards by confirming that their Cloud Service Providers have achieved the FedRAMP Baseline Moderate or Equivalent standard. Currently, to comply with DFARS 252.204-7012, contractors are required to develop a System Security Plan (SSP) and Plan of Action and Milestones (POA&M) detailing the policies and procedures their organization has in place to comply with NIST SP 800-171. The SSP, which outlines the contractor's plan to protect Controlled Unclassified Information (CUI), serves as a foundation for an entity's required NIST SP 800-171 self-assessment. DFARS 252.204-7012 also requires covered DoD contractors to "rapidly report" any "cyber incident" impacting CDI/CUI.

DoD contracts also typically include requirements for NIST SP 800-171 assessments as required by DFARS clauses 252.204-7019 and -7020, which require contractors to have a current Basic, Medium, or High assessment (*i.e.*, not more than three years old) contained in the Supplier Performance Risk System (SPRS) for each covered contractor information system. The highest possible score is 110, which indicates all 110 NIST SP 800-171 security requirements have been fully implemented. A SPRS score of less than 110 indicates security gaps exist. A contractor must create a POA&M identifying security tasks that still need to be accomplished if it scores less than 110.

Moreover, DoD contractors will soon be required to comply with the Cybersecurity Maturity Model Certification (CMMC) Program, as required by DFARS clause 252.204-7021, Cybersecurity Maturity Model Certification Requirements. The CMMC Program provides for the assessment of contractor implementation of cybersecurity requirements to enhance confidence in contactor protection of unclassified information and measure contractors' cybersecurity maturity. The CMMC Program is designed to provide increased assurance to DoD that defense contractors and subcontractors are compliant with information protection requirements for FCI and CUI and are protecting such information at a level commensurate with risk from cybersecurity threats. Once CMMC is fully implemented, DFARS 252.204-7021 will require contractors to achieve the CMMC level required in the relevant DoD contract.

Other agencies may impose their own government-unique cybersecurity requirements. For example, NASA contracts may include separate and distinct security and incident reporting requirements, such as those included in NASA Far Supplement (NFS) 1852.204-76 (Security Requirements for Unclassified Technology Resources) and NFS 1852.223-75 (Major Breach of Safety or Security). Also, the Department of Homeland Security imposes its own unique regulatory requirements for cybersecurity.

Space companies are well-advised to monitor for developments with respect to the ever-evolving government-imposed cybersecurity requirements.

Sourcing and Foreign Contracting Restrictions

Prohibition on Acquisition of Certain Foreign Commercial Satellite Services

Pursuant to statute (10 U.S.C. § 2279), unless an exception is determined to apply in accordance with DFARS 225.772-4, the DoD is prohibited from awarding any contract for commercial satellite services to an offeror that (i) plans to provide the services through a foreign entity that is owned by certain covered foreign countries, or (ii) plans to provide or use launch or other satellite services under contract from such covered foreign countries.[46] The term "covered foreign country" includes China, North Korea, Russia, and any country "that is a state sponsor of terrorism" (a term which currently captures the additional countries of Iran, Sudan, and Syria).[47] DoD is also prohibited from entering into contracts for commercial satellite services with a

foreign entity if doing so "would create an unacceptable cybersecurity risk for DoD."[48] The determination of whether the risk poses one that is "unacceptable" is to be made by the Under Secretary of Defense for Acquisition and Sustainment or the Under Secretary of Defense for Policy.[49]

Additionally, DoD is prohibited from contracting with any entity where the satellite service will be using satellites or launch vehicles designed or manufactured in a covered foreign country or by an entity controlled in whole or in part, or acting on behalf of, the government of a covered foreign country.[50]

"U.S. Commercial Provider" Requirements for "Space Transportation Services"

Pursuant to the Commercial Space Act, with few exceptions, the Government may acquire space transportation services from only "United States commercial [*i.e.*, non-governmental] providers."[51] Also, in planning for space missions, to the maximum extent practicable, the Government must plan the mission to accommodate the "space transportation services" capabilities of "United States commercial providers."[52] The statute defines the term "space transportation services" to mean "the preparation of a space transportation vehicle and its payloads for transportation to, from, or within outer space, or in suborbital trajectory, and the conduct of transporting a payload to, from, or within outer space, or in suborbital trajectory."[53] Regarding the term "United States commercial provider," the statute defines it to mean a commercial provider, organized under the laws of the United States or of a state and that is *more than 50 percent owned by United States nationals*. The term also includes a subsidiary of a foreign company if the Secretary of Transportation finds that:

- such subsidiary has in the past evidenced a substantial commitment to the United States market through—
- investments in the United States in long-term research, development, and manufacturing (including the manufacture of major components and subassemblies); and
- significant contributions to employment in the United States; and
- the country or countries in which such foreign company is incorporated or organized, and, if appropriate, in which it principally conducts its business, affords reciprocal treatment to [United States commercial providers] comparable to that afforded to such foreign company's subsidiary in the United States . . .[54]

Requirement to Buy Star Trackers from American Sources

Star trackers are important satellite components in that they determine the proper location and attitude of the satellite by analyzing the placement of the surrounding stars relative to the payload. Pursuant to 50 U.S.C. § 3239, certain agencies of the U.S. Intelligence Community are prohibited from awarding a contract for a national security satellite if the satellite uses a star tracker that is not produced in the United States, including with respect to both the software and hardware of the star tracker. A waiver may be granted by the agency head where a suitable star tracker is unavailable at a reasonable price or where such waiver is necessary based on an urgent and compelling need in furtherance of national security interests.[55]

Prohibition on Acquisition of Certain Items from Communist Chinese Military Companies (CCMC)

The DoD is required to include DFARS clause 252.225–7007 in solicitations and contracts that involve the delivery of items (including components) covered by the U.S. Munitions List (USML) or the 600 series of the Commerce Control List (CCL). The clause prohibits contractors from delivering under the contract any items covered by the USML or the 600 series of the CCL that are acquired, directly or indirectly, from a CCMC. Regarding the definition of CCMC, the clause broadly defines the term as follows:

Communist Chinese military company means any entity, regardless of geographic location, that is—

- A part of the commercial or defense industrial base of the People's Republic of China (including a subsidiary or affiliate of such entity); or
- Owned or controlled by, or affiliated with, an element of the Government or armed forces of the People's Republic of China.

The clause requires the prime contractor to insert the substance of the clause in all subcontracts for items covered by the USML or the 600 series of the CCL. The related regulations provide that the prohibition does not apply "to components and parts of covered items unless the components and parts are themselves covered by the USML or the 600 series of the CCL."[56] The prohibition may be waived on a case-by-case basis if one of the following individuals determines that a waiver is necessary for national security purposes: (1) the Under Secretary of Defense (Acquisition and Sustainment); (2) the Secretaries of the military departments; or (3) the Component Acquisition Executive of the Defense Logistics Agency.[57]

These prohibitions are being extended by operation of Section 805 of the National Defense Authorization Act for fiscal year 2024. Specifically, Section 805(a)(1)(A) prohibits DoD from entering, renewing, or extending contracts to procure goods, services, or technology with any entity identified on the DoD's list of Chinese military companies or any entity under the control of such entity. Section (a)(1)(B) prohibits DoD from entering, renewing, or extending contracts for "the procurement of goods or services *that include goods or services*" produced or developed by any such entity. DoD's list of Chinese military companies is required by Section 1260H of the fiscal year National Defense Authorization Act, which defines the term ''Chinese military company'' as an entity that is "(i)(I) directly or indirectly owned, controlled, or beneficially owned by, or in an official or unofficial capacity acting as an agent of or on behalf of, the People's Liberation Army or any other organization subordinate to the Central Military Commission of the Chinese Communist Party; or (II) identified as a military-civil fusion contributor to the Chinese defense industrial base; and (ii) engaged in providing commercial services, manufacturing, producing, or exporting."[58]

The Buy American Act

The Buy American Act (BAA) establishes a *preference* for "domestic end products" and "construction material" produced in the United States and provides a price advantage to offerors proposing such items. When it applies, the purchasing agency must impose a pricing penalty on non-U.S. supplies for purposes of bid evaluation only. To purchase foreign-made products, the foreign product's price (with the evaluation penalty) must still be lowest.

Generally, a domestic end product is one that is (i) manufactured in the United States (or a "qualifying country" for DoD procurements); and (ii) the cost of the product's domestic (or qualifying country) components currently must exceed 65 percent of the cost of all the components.[59] (More stringent requirements apply to end products that consist wholly or predominantly of iron or steel.) To qualify as a "domestic component" for purposes of calculating total domestic content of an end product, a component part need only be manufactured in the United States. For "manufactured" components, there is no requirement with regard to the origin, so long as the final manufacturing occurs in the United States (*i.e.*, a component manufactured in the U.S. will be considered "domestic" regardless of the foreign content of its subcomponents). Contracts for COTS items are exempt from the second part of this test and thus need only be manufactured in the United States to comply with the BAA.

For DoD procurements, the DoD treats "qualifying country end products" as domestic end products for purposes of the BAA.[60] A qualifying country end product is an end product manufactured in a qualifying country if –

- The cost of the following types of components exceeds 65 percent of the cost of all its components:
  - Components mined, produced, or manufactured in a qualifying country.
  - Components mined, produced, or manufactured in the United States.
  - Components of foreign origin of a class or kind for which the Government has determined that sufficient and reasonably available commercial quantities of a satisfactory quality are not mined, produced, or manufactured in the United States; or
- The end product is a COTS item.[61]

The list of "qualifying countries" is fairly long and includes Australia, Canada, Finland, France, Germany, Italy, Israel, Japan, Spain, Sweden, Turkey, the United Kingdom, and more.[62]

The BAA generally applies to contracts exceeding the micro-purchase threshold (currently $10,000) but below the Trade Agreements Act (TAA) threshold of (generally) $174,000, for supplies acquired for use in the United States.[63] There are several exceptions, including: (i) unreasonable cost; (ii) public interest; (iii) domestic non-availability; (iv) commercial IT acquisitions; and (v) commissary resale of the product. The BAA provisions do not require flow down to subcontractors; however, even without a mandatory flowdown requirement, prime contractors must still monitor the country of origin of their suppliers' products to ensure their own compliance.

The BAA will continue to apply instead of the TAA even when the purchase is above the TAA threshold for certain categories of products, *including space vehicles and space propulsion units*. However, contractors will need to review the relevant solicitation and resulting contract to confirm the applicable sourcing obligations.

Trade Agreements Act

Although generally less relevant to space-related contracts, where appliable, the TAA expressly *prohibits* contractors from supplying products and services from countries not approved as TAA-eligible, such as China and India.[64] If a product's country of origin (COO) is not TAA-eligible, contractors may not supply that product in connection with TAA-covered procurements absent a government waiver.[65] End products from designated TAA countries will be treated as if they were U.S.-made products for TAA-covered procurements.[66]

To satisfy the TAA's COO requirements, contractors must supply goods that are (a) wholly grown, produced, or manufactured in the United States or a TAA-eligible country; or (b) substantially transformed into new and different articles of commerce in the United States or a TAA-eligible country with names, characters, or uses distinct from that of the article or articles from which they were so transformed.[67] There are several exceptions to the TAA, including: (i) procurements that are set aside for small businesses; (ii) arms, ammunition, war materials, purchases indispensable for national security or national defense; (iii) research and development; (iv) transportation services; (v) utility services; and (vi) certain sole-source acquisitions. If the TAA does not apply because of an exception, the BAA would then apply.[68]

Specialty Metals Restrictions

Unless an exception applies, 10 U.S.C. § 4863 prohibits DoD from acquiring the following items, or any components of the following items, unless any specialty metals contained in the items or components are melted or produced in the United States: aircraft; missile and *space systems*; ships; tank and automotive items; weapon systems; or ammunition. The prohibition extends to specialty metal that is to be purchased directly by the DoD or its prime contractor. "Specialty metals" include: certain steel alloys; nickel, iron-nickel, and cobalt base alloys containing a total of other alloying metals (except iron) in excess of 10%; titanium and titanium alloys; and zirconium and zirconium base alloys.[69] Exceptions to the prohibition include: (i) "de minimis" exception for components; (ii) domestic unavailability; (iii) national security waiver; (iv) acquisitions made outside the U.S. in support of combat or contingency operations; (v) unusual and compelling urgency; (vi) certain COTS acquisitions; (vii) commissary resale; and (viii) acquisition from a "qualifying country" as defined under the BAA.[70]

Certain Prohibition Against Use or Sale of Certain Chinese Telecommunications or Video Surveillance Systems

Federal contractors must also comply with Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Section 889), which seeks to exclude telecommunications equipment and services from Huawei, ZTE, Hytera, Hikvision, and Dahua and their affiliates from the Government supply chain. Specifically, Section 889 requires contractors to represent that:

- It will (or will not) *provide* to the Government covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, in the performance of the contract ("Part A").
- It does (or does not) *use* covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system ("Part B").

The scope of prohibition includes telecommunications and video surveillance equipment and services, such as laptops and desktop computers, modems, printers, phones, physical security devices and access controls, security cameras, services, and network routers and switches. The scope does not include telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

This requirement is implemented in FAR clauses 52.204-24 through -26 and DFARS 252.204-7018. The substance of FAR 52.204-25 (except Part B) and DFARS 252.204-7018, must be in all subcontracts, including subcontracts for the acquisition of commercial products and services.

The Federal Acquisition Supply Chain Security Act of 2018 and the Federal Acquisition Security Council (FASC) Regulation

Section 202 of the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) authorizes the Federal Acquisition Security Council (FASC) to issue recommendations for the exclusion or removal of covered articles or sources. Exclusion orders essentially prohibit contractors from offering or providing excluded articles or services in the performance of a government contract. That is, exclusion orders limit the sources, products, and services that an offeror can propose in response to a solicitation. The FASC will consider a number of "relevant factors" when evaluating covered articles and sources, such as foreign government ownership, control, or influence over the source or covered article as well as other ties between the source and a foreign government. Additional factors include, but are not limited to: (i) the functionality and features of the covered article, including its or its source's access to data and information system privileges; (ii) the user environment in which the covered article is used or installed; (iii) the security, authenticity, and integrity of covered articles and associated supply and compilation chains; (iv) potential or existing threats to or vulnerabilities of Federal systems, programs or facilities, including the potential for exploitability; (v) any transmission of information or data by a covered article to a country outside of the United States;

(vi) implications to government missions or assets, national security, homeland security, or critical functions associated with use of the source or covered article; and (vii) the capacity of the source or the U.S. Government to mitigate risks.

On October 5, 2023, the Federal Acquisition Regulation Council published an interim rule implementing the supply chain security requirements of the FASCSA and a final rule addressing the FASC. Under the interim rule, contractors must comply with exclusion or removal orders for certain products and services as well as share certain supply chain risk information with the U.S. Government. The objective of the interim rule is to "address risks in supply chains by reducing or removing threats and vulnerabilities that may lead to data and intellectual property theft, damage to critical infrastructure, harm to Federal information systems, and otherwise degrade our national security." Consistent with prior supply chain security initiatives, such as the Section 889 ban, the interim rule seeks to make Federal information technology and telecommunications supply chains and information systems more resilient and less vulnerable to threats that could cause disruptions in government operations.

Export Control Requirements

On top of all the above requirements, all contractors are required to comply with a variety of trade laws that prohibit U.S. companies from doing business with certain sanctioned persons and impose requirements on the export of certain types of technology and data. To the extent a contractor receives or creates any export-controlled information in performance of its federal contracts, it may be subject to the cybersecurity requirements addressed above, as well as agency customer-specific and/or contract-specific requirements for safeguarding such information, all in addition to the requirements under the U.S. export control regimes. Defense contractors who manufacture, export, temporarily import, or broker defense articles, or furnish defense services, must comply with the International Traffic in Arms Regulations (ITAR), including registration with the Department of State Directorate of Defense Trade Controls (DDTC). Contractors who export goods not subject to the ITAR (such as commercial items and some defense goods) typically must comply with the Export Administration Regulations (EAR), which includes licensing by the Department of Commerce, Bureau of Industry and Security (BIS).

Code of Conduct and Ethics Restrictions

Space companies and other organizations that conduct business with the U.S. Government must also take heed of strict business ethics and conducts restrictions. The below discussion addresses the most prominent of these restrictions.

Contractor Code of Business Ethics and Conduct

FAR clause 52.203-13, Contractor Code of Business Ethics and Conduct, sets out requirements relating to business ethics and conduct, required compliance systems, and mandatory disclosure of certain violations. Under the clause, if a company receives an award exceeding $6M and has a period of performance greater than 120 days, it must:

- Maintain a written Code of Business Ethics and Conduct, and make a copy available to each employee;
- Establish internal procedures to ensure company and employee compliance with laws and regulations addressing relationships with the U.S. Government or other contractors (*i.e.*, bribery, gift giving, employment of federal employees, collusion, truthful submission, whistleblower protection, etc.);
- Develop a company-wide training program; and
- Disclose to the Government any credible evidence that employees, agents, or subcontractors have violated certain federal criminal laws.

The substance of this clause must be flowed down in subcontracts that exceed $6M on the date of subcontracted award and a performance period of more than 120 days

Bribery and Gratuities

Under the Federal Anti-Bribery Statute, 18 U.S.C. § 201, it is unlawful to give, offer, or promise anything of value, directly or indirectly, to a public official in order to obtain preferential treatment (a bribe) or because of a public act. Also, especially applicable to business development and sales personnel, there are rules that prohibit government employees from receiving (and contractors from giving) a "gratuity". Generally, a gratuity is any favor, discount, entertainment, hospitality, loan, forbearance, or other item or service having monetary value.[71] There are certain exceptions to this gratuity restriction, including: (i) the "20/50" exception, whereby Government employees may accept a gift worth less than $20 per source, per occasion (but with a $50 annual limit); (ii) widely attended gatherings, if a large number of people are expected and the people represent a diversity of views or interests; (iii) gifts based on an established personal relationship; and (iv) gifts based on outside business or employment relationships.

Kickbacks

The Anti-Kickback Act prevents a contractor or a subcontractor from asking for or accepting anything of value (*i.e.*, a kickback) in order to obtain favorable treatment relating to a government contract or subcontract.[72] Specifically, it is prohibited to: (i) offer a kickback; (ii) solicit or accept a kickback; or (iii) include the amount of a kickback in a prime contract or subcontract price. Although commercial item contractors are subject to the Anti-Kickback Act, the applicable FAR clause (52.203-7, Anti-Kickback Procedures) need not be included in commercial item contracts.

Procurement Integrity

The Procurement Integrity Act prohibits contractors from obtaining confidential bid or proposal information of a competitor or the internal source selection information of the U.S. Government prior to the award of a contract because such access could give the contractor an unfair competitive advantage.[73] Specifically, during the conduct of a Federal procurement, company personnel are prohibited from: (i) offering or discussing future employment or business opportunities with any agency procurement official; (ii) offering or giving anything of value to an agency procurement official; or (iii) seeking or obtaining proprietary or source selection information relating to a procurement before contract award.

Revolving Door Restrictions

Space companies and other organizations must also be aware of "revolving door" restrictions prior to hiring any current or former Government officials. Federal law imposes "revolving door" restrictions on former government employees, including a permanent (lifetime) ban prohibiting them from representing others on *particular matters* in which they participated personally and substantially as part of their government duties.[74] The particular matter must be one in which (a) the United States is a party or has a direct and substantial interest; (b) the person participated personally and substantially as an employee or officer at any time in his or her government career; and (c) there was a specific non-Federal party or parties at the time of such participation. Additionally, there is a two-year ban on matters within an individual's official area of responsibility (*e.g.*, direct administrative or operating authority) and a one-year "cooling off period" for "senior"/"very senior" employees.[75] For some former senior-level DoD employees, the contractor is required to obtain an ethics letter from a DoD ethics counselor prior to employment.[76]

Equal Employment Opportunity & Affirmative Action

Government contracts contain socioeconomic requirements to ensure equal employment opportunities without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, disability status, and veteran status. Federal contractors, including those that only provide commercial items, must comply with the Government's socioeconomic policies as set forth in the FAR. The Department of Labor's Office of Federal Contract Compliance Programs is responsible for enforcing contractor compliance with these requirements.

For example, all contractors with total awards in excess of $10,000, including subcontracts, must comply with Equal Employment Opportunity (EEO) procedural and reporting requirements.[77] Contractors must take affirmative action to ensure that applicants are employed, and that employees are treated during employment, in a nondiscriminatory manner. Contractors are also required to provide notices to employees and applicants; to include specific non-discrimination language in employment advertisements, and to send notice of the company's obligations under the EEO contract clause to any labor union with which the company has a collective bargaining agreement. Additional affirmative action requirements apply to veterans and people with disabilities. *See* FAR 52.222-35, *Equal Opportunity for Veterans*, and FAR 52.222-36, *Equal Opportunity for Workers with Disabilities*.

Further, contractors with 50 or more employees that have a contract of $50,000 or more must establish a written affirmative action plan that promotes the hiring of women, minorities, and other protected classes and federally mandated employment practices. If more than $150,000 is received, the plan must also cover certain protected classes of veterans.

These clauses must flow down to subcontractors. The requirements could also apply to a parent company if it has an integrated relationship or "single entity" status with a Government contractor.[78] Single entity status may be found where (i) two entities are under common ownership, with a common board of directors and (ii) the entities have a central corporate office that determines and issues personnel policy for both entities, and generally manages most personnel-related issues for both entities.

Small Business Subcontracting Plan Requirements

To further the Government's long-standing policy of supporting small businesses, prime contractors and subcontractors are expected to offer small business concerns the "maximum practicable opportunity to participate" in subcontracts.[79] Also, if the contractor competes for a contract that exceeds $750,000, the company will be required to propose and, if selected, implement a small business subcontracting plan that includes annual dollar goals—either on a contract-by-contract or company-wide basis—for subcontracting with specified categories of small businesses.[80] The regulations provide for liquidated damages if a company fails to make a good-faith effort to meet its specified subcontract goals.[81] Subcontracting plans are not required from subcontractors when the prime contract contains the clause at FAR 52.212-5, Contract Terms and Conditions Required to Implement Statutes or Executive Orders-Commercial Products and Commercial Services, or when the subcontractor provides a commercial product or service subject to the clause at 52.244-6, Subcontracts for Commercial Products and Commercial Services, under a FAR Part 15 prime contract.

False Claims Act and Mandatory Disclosure

Compliance with the terms of a U.S. Government contract or subcontract is necessary to avoid liability under the False Claims Act ("FCA").[82] The FCA is a punitive tool to discipline federal contractors who defraud the Government. Government contractors may violate the FCA when they falsely represent or certify their compliance with a procurement statute or contract requirement, submit false invoices, or engage in defective pricing with respect to government procurements. Generally, contractors who knowingly submit false claims face potential liability that includes up to treble the Government's damages plus a penalty for each false claim.[83]

For contracts that exceed $5,000,000 and where the performance period is 120 days or more, a contractor must disclose whenever it has "credible evidence" that certain criminal violations or a civil FCA violation occurred in connection with the award, performance, or closeout of one of its government contracts.[84] Likewise, such contractors must disclose "to the Government" when there is a significant overpayment on a contract.

DoD-Specific Requirements that Apply in Certain Circumstances

As discussed above, the Government is increasingly leveraging space technologies that are already in the commercial market. When doing so, the Government is required to use contracting terms and conditions other than those required in FAR Part 15 for traditional government contracts. Where the product or service is not commercial, and FAR Part 15 applies, DoD imposes certain agency-specific statutory and regulatory requirements on contractors and subcontractors. Given the additional burden of these obligations, some space companies may want to avoid FAR Part 15 contracts or form a separate legal entity for its government contracting business, to limit or simplify its exposure to these compliance requirements, as well as to facilitate gaining a facility security clearance (addressed in Section V. below). Several areas of concern to contractors are identified below.

Business System Requirements

Federal procurement regulations and DoD policy require DoD to review the adequacy of a contractor's business systems and to ensure contractors correct identified deficiencies. Contractor business systems include a contractor's accounting; estimating; material management and accounting; purchasing; property management; and earned value management systems.[85] These systems are subject to government audit and resulting penalties to the extent the systems are found to be deficient. These requirements apply to certain FAR Part 15 contracts in excess of applicable dollar thresholds.

Cost Accounting / Cost Principles Compliance

Government contractors that enter FAR Part 15 negotiated contracts may also be required to comply with a series of unique cost accounting rules intended to ensure the Government pays fair and reasonable prices for the goods and services it purchases. Contractors performing cost reimbursement contracts are limited in what costs properly may be charged to the Government—all claimed costs must be allowable, reasonable, and allocable to a particular contract. The cost principles governing the allowability of contract costs are set forth in FAR Part 31. The Cost Accounting Standards (CAS) are a series of accounting principles that govern how a contractor may treat and allocate costs within its accounting system. FAR Part 12 contracts and certain small business contracts are exempt from CAS coverage.[86]

There are two types of CAS coverage: "full" and "modified." A government contractor will be subject to "full" CAS coverage if it receives a single CAS-covered contract valued at more than $50 million, or receives more than $50 million in net CAS-covered awards during a single cost accounting period.[87] Under "full" CAS coverage, all 19 of the standards apply, and the contractor is required to prepare and submit a Disclosure Statement, describing in writing the contractor's cost accounting practices and procedures. "Modified" CAS coverage applies if the contractor receives a single CAS-covered contract valued in excess of $7.5 million and all contracts that are not exempt have not yet reached the threshold for full CAS coverage.[88]

DCAA and DCMA Audits

By entering contracts with the government, a company becomes subject to the government's standard record-keeping and audit requirements.[89] Generally, contractors are required to maintain records pertaining to contract performance for three years following contract completion.

Government contracts are frequently audited and investigated by, among others, Defense Contract Audit Agency (DCAA) and/or Defense Contract Management. Agency (DCMA) auditors. In general, the Government has audit rights for the slew of various contract types. Pursuant to such audits, the government has the right to access and review contractor records; interviews of contractor personnel are also permitted in certain cases.

DCMA is responsible for administering contracts for the DoD and other authorized federal agencies. Through contractor audits, it assures that contractor supplies

and services are delivered on time, at projected cost, and meet all performance requirements. DCAA, on the other hand, has primary responsibility for monitoring and auditing the accounting systems of contractors in doing their work for the DoD. This includes, for example, the following types of audits: (i) accounting system reviews to assess the reliability of a company's accounting data; (ii) rate checks to determine accuracy of indirect cost rates; (iii) incurred cost audits to review cost allocation and allowability; (iv) post-award audits of cost and pricing data; and (v) CAS Disclosure Statement audits.

Facility Security Clearance

For space companies whose solutions and services are used for national security programs, it may become necessary or beneficial for the company to apply for and maintain a Facility Security Clearance (FCL) for the purpose of being able to perform classified work. Contractors may receive FCLs to access classified information under the U.S. National Industrial Security Program ("NISP"). The NISP Operating Manual ("NISPOM") sets out the procedures for contractor safeguarding of classified national security information and continued eligibility for security clearances (in 2021, the NISPOM was finally codified in the Code of Federal Regulations (CFR) at 32 CFR Part 117). The DoD Defense Counterintelligence and Security Agency (DCSA) is responsible for determining DoD contractors' eligibility to access classified information and for inspecting and monitoring contractor compliance with the NISPOM.

Companies must possess an active FCL in order to (i) have access to classified information or (ii) be awarded a classified contract. For corporate entities to be eligible for a FCL: (i) the company must be a U.S. legal entity and located in the U.S.; (ii) the company must have a reputation for integrity and lawful conduct in its business dealings; and (iii) Key Management Personnel (KMPs) as determined by DCSA must have or obtain Personnel Security Clearances (PCLs) at the same classification level as the FCL.

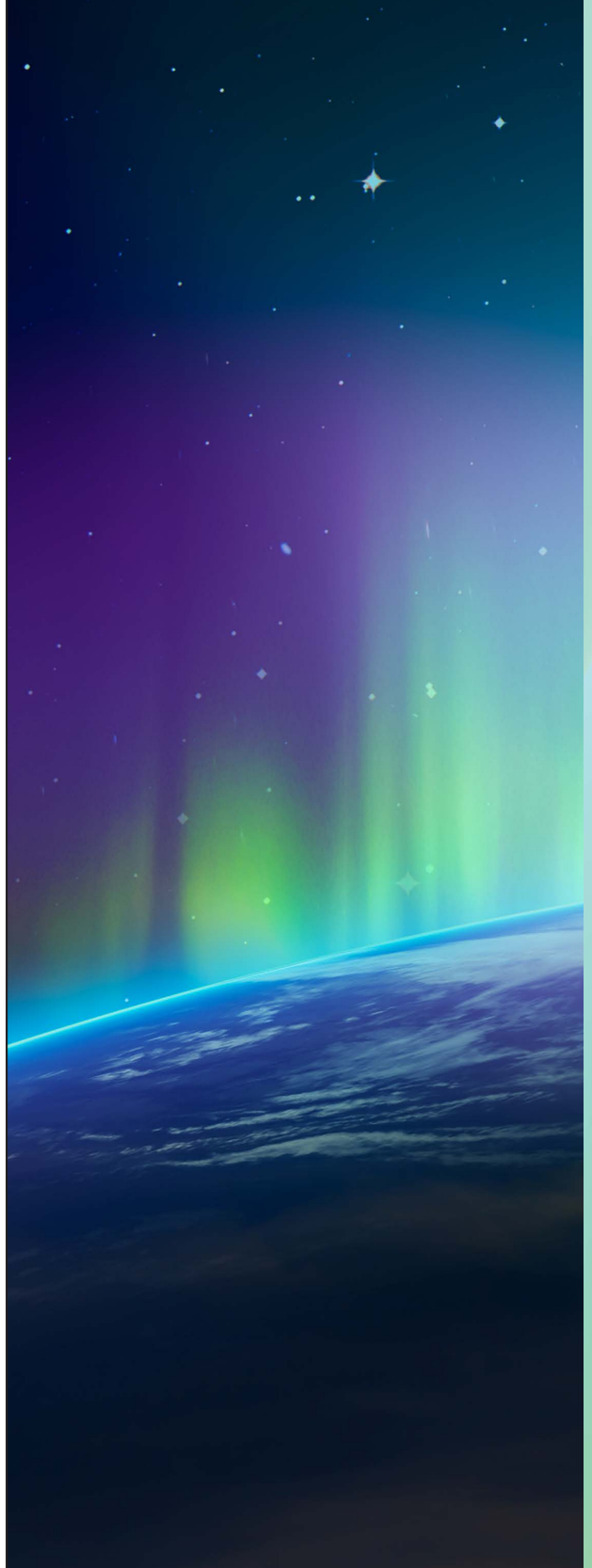
Critically, an entity that is under Foreign Ownership, Control, or Influence (FOCI) is not eligible for a FCL unless the FOCI can be mitigated to DCSA's satisfaction.[90] A U.S. company is considered to be under FOCI whenever a "foreign interest" has the power to direct or decide matters affecting the management or operations of the company in a manner which may result in unauthorized access to classified information or may affect adversely the performance of classified contracts. If DCSA determines that a company is under FOCI, it requires the company to "mitigate" the FOCI through various means, depending on the level and degree of FOCI, in conformity with U.S. national security interests. There are four primary FOCI mitigation measures (from least to most restrictive):

- ***Board Resolution:*** May be appropriate if the foreign interest will not own voting interests sufficient to elect a representative to the company's board, or is otherwise not entitled to board representation. The board must adopt a resolution stipulating: (a) the identification of all foreign shareholders, including the type and number of foreign-owned shares;

(b) acknowledgment of the company's obligation to comply with all industrial security program and export control requirements; and (c) certification that the foreign owner does not require, will not have, and can be effectively prevented from unauthorized access to all classified and export-controlled information entrusted to or held by the company.

- ***Security Control Agreement (SCA):*** May be appropriate if the foreign interest does not effectively own or control the U.S. company, but is entitled to board representation. Under an SCA, the company must appoint at least one Outside Director who has no prior relationship with the company or the foreign interest and is a U.S. citizen; the Outside Director must be approved by the DCSA and have or obtain a PCL. The company must also establish a permanent board committee, the Government Security Committee (GSC) to provide oversight of classified and export-controlled matters.
- ***Special Security Agreement (SSA):*** Used when a U.S. company is effectively owned and controlled by a non-U.S. entity, and the U.S. company needs a FCL at up to the Secret level, although higher level access is possible on a case-by-case basis. By entering into a SSA, the non-U.S. parent agrees that: it will not seek access to or accept US Government classified information entrusted to the company; it will not attempt to control or adversely influence the company's performance of classified contracts; and except as expressly authorized by the SSA, it will limit the parent's involvement in the business affairs of the company to minority participation in the deliberation and decisions of the company's Board of Directors and authorized committees. An SSA requires at least three (3) Outside Directors. Like an SCA, the SSA company must also form a GSC as a permanent board committee.
- *(4) Proxy Agreement:* Generally used when a U.S. company is owned or controlled by a non-U.S. entity and the company needs access to classified information above the Secret level. Under a PA, the voting rights of the non-U.S. owned stock are vested in cleared US citizens approved by DCSA (i.e., the Proxy Holders) who function as the cleared company's Board of Directors (i.e., the Proxy Board). Unlike an SSA, operating under a PA does not impose any restrictions on the company's eligibility to have access to categories of classified information.[91]

The appropriate mitigation measure will depend largely on the extent of the FOCI and the degree of classified work.



Conclusion

The U.S. Government space market offers many opportunities for organizations to contribute to important civilian and national security space endeavors. However, navigating the Government's construct for its transactions with private entities poses significant challenges, including government-unique contracting terms and conditions, strict compliance obligations, and qualification requirements to perform certain types of work. Success in this market requires a balance of innovation, strategic partnerships, and adaptability to evolving policies and priorities. Despite the hurdles, the rewards for those organizations that can effectively navigate these challenges are immense, not only in terms of financial gain but also in advancing national security, economic, and scientific uses of space. As space continues to capture the imagination of nations and individuals alike, the U.S. Government market remains a cornerstone of opportunity and progress for the companies or other organizations daring to reach for the stars.

Endnotes

1 Department of Defense, *Commercial Space Integration Strategy, 2024*, available at *2024 DOD Commercial Space Integration Strategy (defense.gov)*.

2 Joseph Clark, *Space Officials Outline Key Investments Needed to Ensure U.S. Maintains Edge*, May 21, 2024, available at *Space Officials Outline Key Investments Needed to Ensure U.S. Maintains Edge > U.S. Department of Defense > Defense Department News*.

3 U.S. Space Force, Commercial Space Strategy: Accelerating the Purposeful Pursuit of Hybrid Space Architectures, April 8, 2024, available at *https://www.spaceforce.mil//Portals/2/Documents/Space%20Policy/USSF_Commercial_Space_Strategy.pdf*.

4 *See* "Agency Plans and Reports," National Aeronautics and Space Administration, *https://trumpadministration.archives.performance.gov/NASA/#:~:text=The%20National%20Aeronautics%20and%20Space,knowledge%2C%20and%20developing%20new%20technology*.

5 *See* "FY 2024 President's Budget Request Summary," National Aeronautics and Space Administration, *https://www.nasa.gov/wp-content/uploads/2023/03/nasa-fy-2024-cj-v3.pdf*.

6 *See* "How much does the US spend on the Space Force?," USAFacts, *https://usafacts.org/articles/how-much-does-the-us-spend-on-the-space-force/*.

7 *See* "U.S. Space Force Primer," Center for Strategic and International Studies, *https://www.csis.org/analysis/us-space-force-primer*.

8 U.S. Space Force, *Commercial Space Strategy*, supra at 3.

9 *See* SpaceWERX, https://spacewerx.us/.

10 *See* Defense Advanced Research Projects Agency, *https://www.darpa.mil/about-us/about-darpa*.

11 *See* "Years of Innovation," Defense Advanced Research Projects Agency, https://acquisitioninnovation.darpa.mil/years-of-innovation.

12 *See* "Seeking Innovative Concepts for Space Superiority," Defense Advanced Research Projects Agency, https://www.darpa.mil/news-events/2023-09-18

13 The U.S. Government and the space industry are codependent for both the United States and its space industry to maintain their global leadership positions in space. The Government is increasingly leveraging "new commercial space capabilities and services to meet national security requirements" and intends to "deepen the integration of U.S. national security space capabilities and activities with those of our allies and partners." United States Space Priorities Framework at 6 (Dec. 2021), available at *https://www.whitehouse.gov/wp-content/uploads/2021/12/united-states-space-priorities-framework-_-december-1-2021.pdf*

14 *See* United States Government Accountability Office, "National Security Space: Overview of Contracts for Commercial Satellite Imagery," GAO-23-106042 (Dec. 8, 2022), https://www.gao.gov/products/gao-23-106042.

15 DFARS 212.102.

16 51 U.S.C. §§ 20101-20164.

17 51 U.S.C. § 20113(e).

18 *See* NASA Advisory Implementing Instruction, "Space Act Agreements Guide" (last updated Dec. 22, 2023) *https://nodis3.gsfc.nasa.gov/OPD_Docs/NAII_1050_1E_.pdf*.

19 32 C.F.R. § 37.110.

20 *See also* 2 C.F.R. Part 1125, Part 26, Part 28.

21 32 C.F.R. Part 37, Appendix A.

22 15 U.S.C. § 638.

23 31 U.S.C. §§ 1341, 1342.

24 51 U.S.C. § 20148(a).

25 51 U.S.C. § 50915.

26 50 U.S.C. § 1431; FAR 52.250-1

27 FAR 52.102-1(d).

28 FAR 52.250-1(b).

29 *Id.* at (c).

30 DFARS 235.070-2.

31 487 U.S. 500 (1988). The Court's holding in *Boyle* was based on preemption considerations, *i.e.*, because procurement of military equipment is an area of uniquely federal interest, state law holding government contractors liable for design defects in that equipment "does in some circumstances present a 'significant conflict' with federal policy and must be displaced." *Id.* at 512.

32 *Id.* at 512. Courts have interpreted the government contractor defense articulated in *Boyle* as being an extension of *Yearsley* immunity, which is discussed below. *See, e.g.*, *Childs v. San Diego Family Housing LLC*, 22 F.4th 1092, 1097 n.3 (9th Cir. 2022) ("[T]he government contractor defense and derivative sovereign immunity both derived from *Yearsley* . . . the Supreme Court 'planted the seeds of the government contractor defense' in *Yearsley*, before expanding the doctrine in [*Boyle*]" (citations omitted)); *Ollerton v. Nat'l Steel & Shipbuilding Co.*, No. CV 23-1267-MWF(RAOX), 2023 WL 2947544, at *5 (C.D. Cal. Apr. 14, 2023) ("The Court reads *Boyle* as extending *Yearsley* from service to procurement government contracts. In other words, *Boyle* was an outgrowth of *Yearsley* and nothing in Boyle suggests an intent to narrow the protections provided by *Yearsley*. Rather, *Boyle* merely provided a more specific standard to apply where the military is exercising its discretionary function through a contract with a private party.").

33 *Getz v. Boeing Co.*, 654 F.3d 852, 861 (9th Cir. 2011) (citation and internal quotation marks omitted) (emphasis added).

34 *Id.* (citation omitted); *cf. In re World Trade Ctr. Disaster Site Litig.*, 521 F.3d 169, 197 (2d Cir. 2008) ("[I]f the government merely accepted, without substantive review or enforcement authority, decisions made by an entity, that entity would not be entitled to derivative discretionary function immunity [under *Boyle*].").

35 *Turgeon v. Trinity Indus., Inc.*, No. 15-CV-288-PB, 2018 WL 4223165, at *10 (D.N.H. Sept. 5, 2018) (citing cases).

36 *Carley v. Wheeled Coach*, 991 F.2d 1117, 1123–24 (3d. Cir. 1993), *cert. denied*, 510 U.S. 868 (1993) (finding the government contractor defense available to a manufacturer of an ambulance designed for, and sold to, the U.S. General Services Administration but remanding for trial because it was not clear whether the manufacturer had satisfied the third prong of the *Boyle* test).

37 *Burgess v. Colo. Serum Co.*, 772 F.2d 844, 846 (11th Cir. 1985) (pre-*Boyle* case discussing essentially the same three-prong test later articulated in *Boyle*).

38 *Boruski v. United States*, 803 F.2d 1421, 1430 (7th Cir. 1986) (another pre-*Boyle* case involving a vaccine manufacturer and citing *Burgess*, 772 F.2d 844).

39 *See, e.g.*, *Cabalce v. Thomas E. Blanchard & Assocs., Inc.*, 797 F.3d 720, 731 (9th Cir. 2015) ("'In the Ninth Circuit . . . [the government contractor defense] is only available to contractors who

design and manufacture military equipment.'" (citations omitted)).

40 *See, e.g.*, *Hudgens v. Bell Helicopters/Textron*, 328 F.3d 1329, 1333–34 (11th Cir. 2003) ("Although *Boyle* referred specifically to procurement contracts . . . [w]e would be exceedingly hard-pressed to conclude that the unique federal interest recognized in *Boyle*, as well as the potential for significant conflict with state law, are not likewise manifest in a case concerning a 'service contract.'"); *Saleh v. Titan Corp.*, 580 F.3d 1, 9 n.6 (D.C. Cir. 2009) (noting that the court agreed with the Eleventh Circuit that whether *Boyle* applies "is not contingent on whether a contract is for goods or services").

41 *Swift v. Tatitlek Support Servs., Inc.*, No. CV 15-01718-SVW (JPRx), 2016 WL 11604973, at *3 (C.D. Cal. Oct. 26, 2016) (observing that the "*Boyle* decision strongly suggested that the military contractor defense would extend to performance contracts" and therefore applying *Boyle* to a "service contract"); *Laukat v. ABB, Inc.*, No.: CV 19-09436-CJC(Ex), 2019 WL 9088036, at *5 (C.D. Cal. Dec. 13, 2019) ("[I]t would defy the principle of the [government contractor] defense if a defendant-contractor was protected when it produced military equipment subject to reasonably precise federal specifications, but not when the same contractor made repairs to the same equipment subject to the same degree of federal oversight and specifications."); *Ollerton*, 2023 WL 2947544, at *4 (observing that the Ninth Circuit has not yet expressly addressed the question of whether *Boyle* applies to service contractors, noting different district court opinions on this issue, and ultimately concluding *Boyle* does apply to service contractors).

42 Department of Defense, *Commercial Space Integration Strategy*, at 3, supra.

43 *See generally* FAR Subpart 9.4.

44 "Memorandum on Space Policy Directive 5 – Cybersecurity Principles for Space Systems," The White House (Sep. 4, 2020) *https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/.*

45 FAR 4.1903.

46 10 U.S.C. § 2279(a); DFARS 225.772-2.

47 DFARS 225.772-1.

48 10 U.S.C. § 2279(a); DFARS 225.772-2.

49 DFARS 225.772–3.

50 10 U.S.C. § 2279(a); DFARS 225.772-2.

51 51 U.S.C. § 50131.

52 *Id*.

53 51 U.S. Code § 50101(4).

54 51 U.S. Code § 50101(7)(B).

55 50 U.S.C. § 3239.

56 *See* DFARS 225.770-2.

57 *See* DFARS 225.770-5.

58 Section 1260H(d)(1) of the National Defense Authorization Act for Fiscal Year 2021, P.L. 116-283.

59 FAR 25.003.

60 DFARS 252.225-7000(b)(2).

61 DFARS 252.225-7001.

62 *Id*.

63 FAR 25.1101.

64 *See generally*, FAR Part 25.4.

65 Government agencies have discretion to issue waivers for unavailability (where no equivalent product is available from a designated country). DoD may issue a national interest waiver where a "purchase by an overseas purchasing activity of products critical to the support of U.S. forces stationed abroad." DFARS 225.403(ii).

66 FAR 25.403(c).

67 19 U.S.C. § 2518(4)(B); FAR 25.003.

68 FAR 25.401.

69 10 U.S.C. § 4863(l).

70 *See generally*, 10 U.S.C. § 4863.

71 5 C.F.R. § 2635.203(b).

72 41 U.S.C. §§ 51-58.

73 41 U.S.C. §§ 2101-2107 (formerly § 423(b)).

74 18 U.S.C. § 207(a)(1).

75 *See* 18 U.S.C. § 207(a)(2) and § 207(c), respectively.

76 DFARS 252.203-7000.

77 *See* FAR 52.222-26.

78 The single entity test looks at five factors: (1) The entities have common ownership; (2) The entities have common directors and/or officers; (3) One entity has de facto day-to-day control over the other through policies, management, or supervision of the entity's operations; (4) The personnel policies of the entities emanate from a common or centralized source; and (5) The operations of the entities are dependent on each other, e.g., services are provided principally for the benefit of one entity by another and/or both entities share management, offices, or other services.

79 *See* FAR 52.219-8.

80 *See* FAR 52.219-9.

81 FAR 52.219-16.

82 31 U.S.C. §§ 3729 *et seq*.

83 31 U.S.C. § 3729(a); 28 C.F.R. § 85.3.

84 *See* FAR 52.203-13.

85 DFARS 252.242-7005.

86 *See* 48 C.F.R. Ch. 99.

87 *See* 48 C.F.R. § 9903.201-2(a).

88 Modified CAS coverage requires contractors to comply only with (1) CAS 401, Consistency in Estimating, Accumulating, and Reporting Costs; (2) CAS 402, Consistency in Allocating Costs Incurred for the Same Purpose; (3) CAS 405, Accounting for Unallowable Costs; and (4) CAS 406, Cost Accounting Standard – Cost Accounting Period.

89 FAR 52.215-2.

90 DCSA has published a useful FAQ on FOCI: "FAQs," (Defense Security Service), available at *https://www.dss.mil/ma/ctp/isia/bams/foci/foci_faqs/*.

91 An SSA allows the cleared contractor access to classified information up to the SECRET classification level *only*. The SSA company would separately have to obtain a National Interest Determination (NID) for access to TOP SECRET classified information or any other categories of "proscribed information" (e.g., Communications Security (COMSEC); Restricted Data (RD); Special Access Program (SAP) information; and Sensitive Compartmented Information (SCI)).

Alicante
Amsterdam
Baltimore
Beijing
Berlin
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dublin
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Munich
New York
Northern Virginia
Paris
Philadelphia
Riyadh
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Warsaw
Washington, D.C.

*Our associated offices

www.hoganlovells.com